

DOCKET NO.: MSFT-0135/147325.1
Application N .: 09/525,510
Office Action Dated: November 13, 2003

**PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116**

REMARKS/ARGUMENTS

The following Request for Reconsideration After Final is submitted in response to the Final Office Action issued on November 13, 2003 (Paper No. 9(?)) in connection with the above-identified patent application, and is being filed within the three-month shortened statutory period set for a response by the Final Office Action.

Claims 1-46 remain pending in the present application, and stand rejected. Applicants again respectfully request reconsideration and withdrawal of the rejection of the claims, consistent with the following remarks.

The Examiner has again rejected claims 1-46 under 35 USC § 103(a) as being obvious over Matsuzaki et al. (U.S. Patent No. 6,058,476) in view of Patel (U.S. Patent No. (6,374,355)). Applicants respectfully traverse the § 103(a) rejection of such claims.

As was previously set forth, independent claim 1 recites a method for releasing digital content to a rendering application, where the rendering application forwards the digital content to an ultimate destination by way of a path therebetween. Significantly, the path is defined by at least one module and the digital content is initially in an encrypted form.

In the method, an authentication of at least a portion of the path is performed to determine whether each defining module thereof is to be trusted to appropriately handle the digital content passing therethrough. If in fact each such defining module is to be trusted based on the authentication, the encrypted digital content is decrypted and forwarded to the rendering application for further forwarding to the ultimate destination by way of the authenticated path.

Independent claim 24 recites substantially the same subject matter as claim 1, albeit as a computer-readable medium having computer-executable instructions thereon that perform the method.

Once again, with the present invention, encrypted content is decrypted and released to a rendering application only after an authentication determines that trust may be imparted to the path that the rendering application will employ to forward the decrypted content to the ultimate destination. To summarize, then, the present invention requires –

- (1) a rendering application forwarding digital content to an ultimate destination by way of a path therebetween, where the path is defined by at least one module;
- (2) an authentication of the path; and
- (3) a decryption and forwarding of decrypted content through the path, but only if the authentication succeeds.

The rendering application may be any application that renders content, such as an audio player rendering audio from audio content, a video player rendering video from video content, a visual renderer rendering a picture from picture content, or the like. Significantly, the path is not merely a wire or a communications channel, but is defined by interconnected modules, such as for example audio filters, video filters, picture filters, and the like. Also significantly, inasmuch as the content passing through the modules / filters that define the path is to be decrypted content, such modules / filters of the path must be trusted to handle the decrypted content in a trusted manner, and are therefore each authenticated to determine trustworthiness. Such trust is for example with regard to the fact that the modules / filters defining the path will not copy the decrypted content for nefarious purposes. As may be appreciated, in the course of being authenticated, a particular module may prove its

trustworthiness by, for example, proffering a digital certificate issued by an entity that may itself be deemed to be trustworthy. Thus, and again, the present invention is especially useful when the encrypted content is of a type that should not be copied in a decrypted form, such as for example copyright-protected audio and/or video and/or picture content.

Once again, the Matsuzaki reference discloses a method of encrypting content for transmission between a first and a second device, where the first device encrypts the content and then transmits same to the second device in the encrypted form for decryption thereby. According to the Examiner, the communications path is represented in the Matsuzaki reference by a cable 116 such as that shown in Fig. 9 which connects a first device 110 (a disc player) and a second device 111 (a computer), and also by a SCSI controller 121 in the computer 110 (Fig. 10). However, and as was previously set forth, the Matsuzaki reference is clear that all communications between the first device and the second device thereof are *encrypted*. Thus, the Matsuzaki reference does not disclose or suggest *decrypting* the encrypted digital content and forwarding such *decrypted* content over the particular path identified by the Examiner or any authenticated path, as is required by claims 1 and 24.

The Examiner notes in a Response to Arguments section at page 10 of the Office Action that the Matsuzaki reference does disclose decrypting content (cj) at a second encryption IC 56 (Fig. 3) and sending such decrypted content to an MPU 55. However, and significantly, such decrypted content is not disclosed or suggested as being sent by a rendering application as is required by claims 1 and 24, and is not disclosed or suggested as being forwarded to an ultimate destination by way of a path therebetween, where the path is defined by at least one module, as is also required by claims 1 and 24. Instead, such decrypted content cj is shown and disclosed as being sent directly from the second encryption

IC 56 to the MPU 55 without any path-defining intermediate modules therebetween. Further, inasmuch as the decrypted content *cj* is not sent by way of path-defining intermediate modules, no authentication of such a path is disclosed or suggested, as is required by claims 1 and 24, nor is decryption and forwarding of the decrypted content *cj* through the path, but only if the authentication succeeds, disclosed or suggested, as is required by claims 1 and 24.

Moreover, Applicants respectfully submit that the decrypted content *cj* pointed to by the Examiner in the Matsuzaki reference is disclosed as traveling a different route other than the path pointed to by the Examiner in the Matsuzaki reference, and therefore cannot be employed to show that the Matsuzaki reference discloses or suggests *decrypted* content being transmitted through an *authenticated* path defined by at least one module, as is required by claims 1 and 24.

Once again, the Matsuzaki reference would not disclose or suggest *decrypted* content being transmitted through an *authenticated* path defined by at least one module, as is required by claims 1 and 24, for the reason that the Matsuzaki reference need not authenticate any sensitive path such as that between first and second devices 51, 52 of Fig. 3, when the content transmitted along such path is *encrypted*. To summarize, then, whereas claims 1 and 24 require both authenticating a path and sending decrypted content over the authenticated path, Matsuzaki discloses only authenticating a destination or source and sending / receiving encrypted content to / from the authenticated destination or source.

In making the present rejection, the Examiner admits that Matsuzaki fails to disclose or suggest authenticating any portion of the Matsuzaki path. Nevertheless, the Examiner continues by arguing that the Patel reference discloses authenticating at least a portion of a path. Such Patel reference discloses in connection with a wireless

communications system that a mobile unit and a base network mutually establish secure over-air communications therebetween by way of exchanging data and then mutually deriving a cryptographic key based on such exchanged data. Such key is then employed to establish encrypted communications channels by which the mobile unit and the base network communicate.

Like the Matsuzaki reference, then, the Patel reference does not disclose or suggest decrypting encrypted digital content and forwarding such decrypted content through a path *comprising pre-defined modules*, as is required by claims 1 and 24. As with the Matsuzaki reference, the Patel reference discloses that the path need not be trusted because the content is encrypted while traversing such path. Thus, and again, whereas claims 1 and 24 require both authenticating a path comprising pre-defined modules and sending decrypted content over the authenticated path, both Patel and Matsuzaki disclose only authenticating a destination or source and sending / receiving encrypted content to / from the authenticated destination or source.

Moreover, the Patel reference does not even disclose or suggest that the Patel path is defined by modules through which the Patel data passes, as is the case with claims 1 and 24. Instead, in the Patel reference, the path is merely one or more ethereal over-air communications channels.

Once again, Applicants respectfully submit that both the Matsuzaki and Patel references teach only that first and second devices authenticate each other, and not a path defined by modules therebetween. Moreover, such references would not teach that either of such first and second devices authenticates such a module-defining path therebetween for the

DOCKET NO.: MSFT-0135/147325.1
Application No.: 09/525,510
Office Action Dated: November 13, 2003

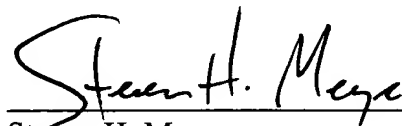
PATENT
REPLY FILED UNDER EXPEDITED
PROCEDURE PURSUANT TO
37 CFR § 1.116

reason that the Matsuzaki or Patel content traverses non-module-defining paths and is
encrypted.

Thus, Applicants respectfully submit that neither the Matsuzaki reference nor the Patel references disclose (1) an authentication of a path defined by at least one module and (2) a decryption and forwarding of content through such a path, but only if the authentication succeeds, as is required by claims 1 and 24. Accordingly, and for all the aforementioned reasons, Applicants respectfully submit that the Matsuzaki reference and the Patel reference cannot be combined to make obvious claims 1 or 24, or any claims depending therefrom, including claims 2-23 and 25-46. Thus, Applicants respectfully request reconsideration and withdrawal of the § 103(a) rejection.

In view of the foregoing discussion, Applicants respectfully submit that the present application, including claims 1-46, is in condition for allowance, and such action is respectfully requested. Should the Examiner disagree, Applicants respectfully request that the Examiner telephone the undersigned at the number below to discuss the claims.

Date: January 22, 2004



Steven H. Meyer
Registration No. 37,189

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439